PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2001-051903**
(43)Date of publication of application : **23.02.2001**

(51)Int.Cl. **G06F 12/14**
G06F 12/00
G06K 17/00
G06K 19/073

(21)Application number : **11-222351**
(22)Date of filing : **05.08.1999**

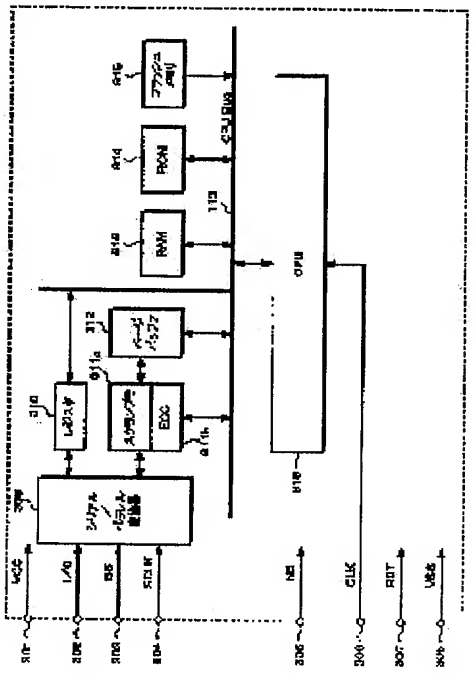
(71)Applicant : **SONY CORP**
(72)Inventor : **IMURA SHIGERU**

(54) SEMICONDUCTOR STORAGE DEVICE AND OPERATION SETTING METHOD FOR SEMICONDUCTOR STORAGE DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To increase security and to obtain compatibility with memory cards now in use by providing a ciphering means which ciphers data stored in a nonvolatile semiconductor memory and a control means which controls the ciphering.

SOLUTION: Serial data are converted into parallel data in a serial/parallel converter 309 through a bidirectional data communication line I/O between a memory stick which is made intelligent and an external device. To cipher and store the data, a scrambler 311a is supplied with plaintext data and a cipher key and generates ciphered data through specific ciphering algorithm and finally stores them in a flash memory 315. The data are possibly not ciphered and stored in the flash memory 315 in the form of the plaintext data when necessary. Thus, the data are ciphered and stored in the flash memory 315, so the security of the stored data is enhanced.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－51903
（P2001－51903A）
(43)公開日　平成13年２月23日(2001.2.23)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
			３２０Ｃ	５Ｂ０３５
	３１０		３１０Ｅ	５Ｂ０５８
			３１０Ｋ	５Ｂ０８２
12/00	５３７	12/00	５３７Ｈ	

審査請求　未請求　請求項の数38　ＯＬ　（全 21 頁）　最終頁に続く

(21)出願番号　特願平11－222351

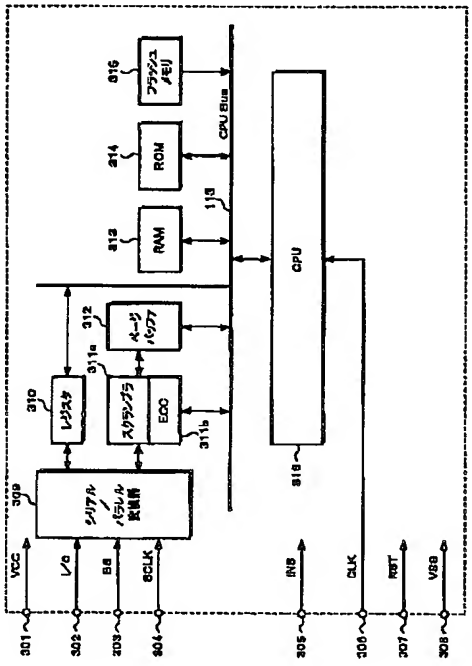
(22)出願日　平成11年８月５日(1999.8.5)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　井村　滋
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082762
弁理士　杉浦　正知

最終頁に続く

(54)【発明の名称】　半導体記憶装置及び半導体記憶装置の動作設定方法

(57)【要約】
【課題】　セキュリティを高めることができると共に、現行のメモリカードとの互換性を図れるようにした半導体記憶装置及び半導体記憶装置の動作設定方法を提供する。
【解決手段】　メモリスティックの構成のメモリカードに、ＣＰＵと、暗号化回路が設けられる。入出力されるデータは、暗号化されて、フラッシュメモリに記憶される。メモリスティックをアクセスするための命令体系には、公開された命令体系と非公開の命令体系とを有している。フラッシュメモリに記憶されるファイルデータは、各ファイルデータ毎に、アクセス制限、コピーガード情報、及びアクセス時の暗号化、暗証番号を選択的に設定できる。これらのファイルデータは、隠されたデータファイルを含むデータファイルが処理を管理している。また、ファイルデータにはアクセス権が設定され、アクセス権に従って、ファイルデータの読み出し及び書き込みのアクセスが制限される。このように、データが暗号化されてフラッシュメモリに記憶されるため、記憶されるデータのセキュリティが強化される。



【特許請求の範囲】

【請求項1】 不揮発性半導体メモリと、上記不揮発性半導体メモリに対するデータの入出力の制御を行なうデータ入出力制御手段と、外部機器とのインターフェース手段とからなるメモリカードの構成の半導体記憶装置に対して、上記不揮発性半導体メモリに記憶するデータを暗号化する暗号化手段と、上記暗号化を制御する制御手段とを設けるようにした半導体記憶装置。

【請求項2】 上記不揮発性メモリをアクセスするための命令体系には、公開された命令体系と非公開の命令体系とを有するようにした請求項1に記載の半導体記憶装置。

【請求項3】 上記不揮発性半導体メモリに記憶されるファイルデータは、隠されているファイルデータを含む請求項1に記載の半導体記憶装置。

【請求項4】 上記不揮発性半導体メモリに記憶されるファイルデータは、各ファイルデータ毎に、アクセス制限、コピーガード情報、及びアクセス時の暗号化、暗証番号を選択的に設定できるようにした請求項1に記載の半導体記憶装置。

【請求項5】 上記不揮発性半導体メモリに記憶されるファイルデータは、隠されたデータファイルを含むデータファイルが処理を管理するようにした請求項4に記載の半導体記憶装置。

【請求項6】 上記不揮発性半導体メモリに記憶されるファイルデータにはアクセス権が設定され、上記アクセス権に従って、上記ファイルデータの読み出し及び書き込みのアクセスが制限される請求項1に記載の半導体記憶装置。

【請求項7】 上記アクセス権の制限は、ユーザの暗証番号により設定できる請求項1に記載の半導体記憶装置。

【請求項8】 上記制御手段の作動クロックと、データ入出力に使用される転送クロックが独立して変更可能とされた請求項1に記載の半導体記憶装置。

【請求項9】 上記制御手段の作動クロックを分周して、データ入出力の転送クロックとして使用するようにした請求項1に記載の半導体記憶装置。

【請求項10】 上記暗号化手段は、個人情報のパラメータに基づいて暗号化キーを発生するようにした請求項1に記載の半導体記憶装置。

【請求項11】 上記暗号化手段は、ユーザの暗証番号に基づいて暗号化キーを発生するようにした請求項1に記載の半導体記憶装置。

【請求項12】 上記暗号化手段は、加入者番号に基づいて暗号化キーを発生するようにした請求項1に記載の半導体記憶装置。

【請求項13】 上記暗号化手段は、上記個人情報のパラメータと、上記非公開の管理用の命令体系でアクセスされるパラメータに基づいて暗号化キーを発生するようにした請求項1に記載の半導体記憶装置。

【請求項14】 上記暗号化手段は、暗号化アルゴリズムにより生成された暗号化キーと変化する値とを複合した値を暗号化キーとするようにした請求項1に記載の半導体記憶装置。

【請求項15】 上記変化する値は、ページモードをアクセスする際のページ番号である請求項14に記載の半導体記憶装置。

【請求項16】 上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出されたデータを解読して出力するようにした請求項1に記載の半導体記憶装置。

【請求項17】 上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出されたデータを解読して出力するモードと、上記不揮発性半導体メモリに入力データをそのまま記憶すると共に上記不揮発性半導体メモリから読み出されたデータをそのまま出力するモードとが設定可能とされた請求項1に記載の半導体記憶装置。

【請求項18】 上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出されたデータを解読して出力するモードと、上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出された暗号化されたデータを出力するモードを備えるようにした請求項1に記載の半導体記憶装置。

【請求項19】 上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出されたデータを解読して出力するモードと、上記不揮発性半導体メモリに入力データをそのまま記憶すると共に上記不揮発性半導体メモリから読み出されたデータをそのまま出力するモードと、上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出された暗号化されたデータを出力するモードを備えるようにした請求項1に記載の半導体記憶装置。

【請求項20】 不揮発性半導体メモリと、上記不揮発性半導体メモリに対するデータの入出力の制御を行なうデータ入出力制御手段と、外部機器とのインターフェース手段とからなるメモリカードの構成の半導体記憶装置に対して、データを暗号化し、上記暗号化されたデータを上記不揮発性半導体メモリに記憶するようにした半導体記憶装置の動作設定方法。

【請求項21】 上記不揮発性メモリをアクセスするための命令体系には、公開された命令体系と非公開の命令体系とを有するようにした請求項20に記載の半導体記憶装置の動作設定方法。

【請求項22】 上記不揮発性半導体メモリに記憶されるファイルデータは、隠されているファイルデータを含む請求項20に記載の半導体記憶装置の動作設定方法。

【請求項２３】 上記不揮発性半導体メモリに記憶されるファイルデータは、各ファイルデータ毎に、アクセス制限、コピーガード情報、及びアクセス時の暗号化、暗証番号を選択的に設定できるようにした請求項２０に記載の半導体記憶装置の動作設定方法。

【請求項２４】 上記不揮発性半導体メモリに記憶されるファイルデータは、隠されたデータファイルを含むデータファイルが処理を管理するようにした請求項２３に記載の半導体記憶装置の動作設定方法。

【請求項２５】 上記不揮発性半導体メモリに記憶されるファイルデータにはアクセス権が設定され、上記アクセス権に従って、上記ファイルデータの読み出し及び書き込みのアクセスが制限される請求項２０に記載の半導体記憶装置の動作設定方法。

【請求項２６】 上記アクセス権の制限は、ユーザの暗証番号により設定できる請求項２０に記載の半導体記憶装置の動作設定方法。

【請求項２７】 上記制御手段の作動クロックと、データ入出力に使用される転送クロックが独立して変更可能とされた請求項２０に記載の半導体記憶装置の動作設定方法。

【請求項２８】 上記制御手段の作動クロックを分周して、データ入出力の転送クロックとして使用するようにした請求項２０に記載の半導体記憶装置の動作設定方法。

【請求項２９】 上記暗号化手段は、個人情報のパラメータに基づいて暗号化キーを発生するようにした請求項２０に記載の半導体記憶装置の動作設定方法。

【請求項３０】 上記暗号化手段は、ユーザの暗証番号に基づいて暗号化キーを発生するようにした請求項２０に記載の半導体記憶装置の動作設定方法。

【請求項３１】 上記暗号化手段は、加入者番号に基づいて暗号化キーを発生するようにした請求項２０に記載の半導体記憶装置の動作設定方法。

【請求項３２】 上記暗号化手段は、上記個人情報のパラメータと、上記非公開の管理用の命令体系でアクセスされるパラメータに基づいて暗号化キーを発生するようにした請求項２０に記載の半導体記憶装置の動作設定方法。

【請求項３３】 上記暗号化手段は、暗号化アルゴリズムにより生成された暗号化キーと変化する値とを複合した値を暗号化キーとするようにした請求項２０に記載の半導体記憶装置の動作設定方法。

【請求項３４】 上記変化する値は、ページモードをアクセスする際のページ番号である請求項３３に記載の半導体記憶装置の動作設定方法。

【請求項３５】 上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出されたデータを解読して出力するようにした請求項２０に記載の半導体記憶装置の動作設定方法。

【請求項３６】 上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出されたデータを解読して出力するモードと、上記不揮発性半導体メモリに入力データをそのまま記憶すると共に上記不揮発性半導体メモリから読み出されたデータをそのまま出力するモードとが設定可能とされた請求項２０に記載の半導体記憶装置の動作設定方法。

【請求項３７】 上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出されたデータを解読して出力するモードと、上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出された暗号化されたデータを出力するモードを備えるようにした請求項２０に記載の半導体記憶装置の動作設定方法。

【請求項３８】 上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出されたデータを解読して出力するモードと、上記不揮発性半導体メモリに入力データをそのまま記憶すると共に上記不揮発性半導体メモリから読み出されたデータをそのまま出力するモードと、上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出された暗号化されたデータを出力するモードを備えるようにした請求項２０に記載の半導体記憶装置の動作設定方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、特に、ネットワークを介して配信されてくるコンテンツのデータを保存するのに用いて好適な半導体記憶装置及び半導体記憶装置の動作設定方法に関する。

【０００２】

【従来の技術】インターネットを使って、音楽データを配信するようなサービスが開始されている。このようなサービスでは、インターネット上に、音楽データを配信するようなサイトが設けられる。ユーザはこのサイトをアクセスして、所望の楽曲を選択すると、選択された音楽データがインターネットを介して送られ、記録媒体にダウンロードされる。

【０００３】また、ディジタル衛星放送を使って音楽配信を行なうようなサービスが提案されている。このようなサービスでは、音楽チャンネルで、その番組を提供する映像データや音声データと共に、付加データとして、ダウンロード用の音楽データと、ダウンロード用の画面を形成するためのMHEG (Multimedia and Hypermedia Information Coding Experts Group) やXML (eXtensible Markup Language) 等のスクリプト言語のデータが送られてくる。このスクリプト言語のデータにより、ダウンロード用の画面が形成され、この画面上から指示

を与えると、ダウンロード用として送られてきた音楽データが記録媒体にダウンロードされる。

【０００４】更に、携帯電話を使って音楽配信を行うようにしたサービスが提案されている。このようなサービスでは、携帯電話に音楽配信サービスを提供するダイアルが設けられる。携帯電話で所定のダイアル番号に接続すると、音楽データの配信サービスを受けることができる。携帯電話を操作すると、所望の音楽データが携帯電話の回線網を介して送られ、この音楽データが携帯電話に装着された記録媒体にダウンロードされる。

【０００５】

【発明が解決しようとする課題】このように、インターネットやディジタル衛星放送、携帯電話回線等、種々の伝送媒体を使って、音楽データ、出版物、ゲームのソフトウェア等のコンテンツを提供するサービスが考えられている。そして、このようなサービスでは、送られてきたデータが記録媒体にダウンロードされる。

【０００６】このように、コンテンツのデータをダウンロードするための記録媒体としては、フロッピディスクやハードディスク等の磁気ディスク、或いは、ＣＤ－Ｒ（CD-Recordable）やMO（Magneto-Optical）のような光ディスク又は光磁気ディスクを用いることが考えられる。ところが、このようなディスク状の記録媒体は、機構部を含むため、耐震性に問題があり、また、大型化し、外部に携帯したり、手軽に使用するのは困難である。

【０００７】そこで、このようなコンテンツのデータをダウンロードするための記録媒体として、メモリスティックと称されるメモリカードを用いることが提案されている。

【０００８】メモリスティックは、ＮＡＮＤ型のフラッシュメモリを用いたカード型の不揮発性半導体メモリである。このメモリスティックは、従来から広く使われているＰＣＭＣＩＡ（Personal Computer Memory Card International Association）インターフェースを利用したパラレルインターフェースではなく、シリアルの半二重同期データ転送方式を利用して２０ＭＢ／ｓ程度のアクセス速度を有しており、高速アクセスが可能で、メモリ容量もおよそ６４ＭＢ程度まで計画されている。この６４ＭＢというメモリスティックの容量は、既存のフロッピディスクの記憶容量（１．４ＭＢ）よりも大きく、コンテンツのデータを記録するのには十分な容量であると考えられる。また、この容量は、MD（Mini Disc）やＣＤ－Ｒの記憶容量（１２８ＭＢから６４０ＭＢ）より小容量ではあるが、ＭＤやＣＤ－Ｒは機構部を含み大型化し、手軽に扱えないのに対して、メモリスティックは、小型で扱いが容易であり、耐震性に優れている。

【０００９】例えば、音楽データをダウンロードするような場合には、ユーザは、このダウンロードした音楽データを携帯型のヘッドホンステレオで再生したり、カーオーディオで再生することが考えられる。このような使用方法では、小型で、耐震性が優れたメモリスティックは、非常に有用の記録媒体であると考えられる。

【００１０】ところが、メモリスティックは、現状では、ＣＰＵは内蔵されておらず、セキュリティ機能が万全であるとは言えない。音楽データをダウンロードするような場合には、著作権を保護する上から、セキュリティを高める必要がある。特に、ネットワークを利用してこれらのコンテンツのデータを取得する際に、電子マネーを使って、課金を行なうことが考えられている。メモリスティックでは、ＣＰＵが内蔵されていないため、このような課金処理が困難である。

【００１１】また、ＣＰＵが内蔵されたカードとしては、ＩＣカードが知られている。例えば、ヨーロッパのＧＳＭ（Group Special Mobile）方式の携帯電話では、ＩＳＯ７８１６に準拠したＳＩＭと呼ばれるＩＣカードが用いられている。このＩＣカードは、ＧＳＭ方式の携帯電話で、認証、契約内容、暗号アルゴリズム、短縮ダイアル等を記憶するのに使われている。また、ペイテレビジョンや、モンデックスシステムのような電子マネーで、ＣＰＵ内蔵のＩＣカードが使われている。このようなＩＣカードは、メモリカードに比較して、複製、偽造に対して高い守秘性がある。

【００１２】しかしながら、これらのＩＣカードは、メモリ容量が小さく、アクセス速度も遅いため、ダウンロードしたコンテンツを保存しておくような用途に使用することは困難である。

【００１３】したがって、この発明の目的は、セキュリティを高めることができると共に、現行のメモリカードとの互換性を図れるようにした半導体記憶装置及び半導体記憶装置の動作設定方法を提供することにある。

【００１４】

【課題を解決するための手段】この発明は、不揮発性半導体メモリと、不揮発性半導体メモリに対するデータの入出力の制御を行なうデータ入出力制御手段と、外部機器とのインターフェース手段とからなるメモリカードの構成の半導体記憶装置に対して、不揮発性半導体メモリに記憶するデータを暗号化する暗号化手段と、暗号化を制御する制御手段とを設けるようにした半導体記憶装置である。

【００１５】この発明は、不揮発性半導体メモリと、不揮発性半導体メモリに対するデータの入出力の制御を行なうデータ入出力制御手段と、外部機器とのインターフェース手段とからなるメモリカードの構成の半導体記憶装置に対して、データを暗号化し、暗号化されたデータを不揮発性半導体メモリに記憶するようにした半導体記憶装置の動作設定方法である。

【００１６】メモリスティックの構成のメモリカードに、ＣＰＵと、暗号化回路が設けられる。そして、入出力されるデータは、暗号化されて、フラッシュメモリに

記憶される。また、メモリスティックをアクセスするための命令体系には、公開された命令体系と非公開の命令体系とを有している。フラッシュメモリに記憶されるファイルデータは、各ファイルデータ毎に、アクセス制限、コピーガード情報、及びアクセス時の暗号化、暗証番号を選択的に設定できる。これらのファイルデータは、隠されたデータファイルを含むデータファイルが処理を管理している。また、ファイルデータにはアクセス権が設定され、アクセス権に従って、ファイルデータの読み出し及び書き込みのアクセスが制限される。このように、データが暗号化されてフラッシュメモリに記憶されるため、記憶されるデータのセキュリティが強化される。

【００１７】

【発明の実施の形態】この発明の実施の形態について以下の順序で説明する。

【００１８】１．ＳＩＭの内部構成

２．メモリスティックの内部構成

３．スマートスティックの一例

３－１．スマートスティックの一例の構成

３－２．外部装置とスマートスティックとのセッション

３－３．暗号化について

３－４．ファイル構成について

３－５．アクセス処理について

４．インテリジェント化されたメモリスティックの他の例。

【００１９】１．ＳＩＭの内部構成

この発明は、ＳＩＭと呼ばれるＩＣカードの機能をメモリスティックと呼ばれるメモリカードに付加することで、セキュリティを高めることができると共に、現行のメモリスティックとの互換性を図れるようにしたものである。本願の説明に先立ち、ＳＩＭと呼ばれるＩＣカードと、メモリスティックと呼ばれるメモリカードについて説明する。

【００２０】ＳＩＭと呼ばれるＩＣカードは、ＩＳＯ（International Organzation for Standardization）７８１６に準拠したＣＰＵ内蔵のＩＣカードであり、ＧＳＭ（Group Special Mobile）方式の携帯電話で、加入者の暗唱番号により認証、契約内容暗号アルゴリズム、短縮ダイアル番号等を記憶するのに用いられている。

【００２１】図１はＳＩＭと呼ばれるＩＣカードの内部構成を示すブロック図である。このＩＣカードには、外部機器との接続端子として、電源端子１０１と、プログラム用電源端子１０２と、双方向データの入出力端子１０３と、クロック入力端子１０４と、リセット入力端子１０５と、接地端子１０６とが設けられる。

【００２２】電源端子１０１は、作動電源Ｖccを外部から供給するためのものである。作動電源Ｖccの電圧は５Ｖ或いは３Ｖである。

【００２３】プログラム電源端子１０２は、内蔵されているＥＥＰＲＯＭ（Electrically Erasable and Programmable ROM）１１０に、プログラム用電源Ｖppを供給するためのものである。ＥＥＰＲＯＭ１１０は、電子的消去可能な不揮発性メモリである。このＥＥＰＲＯＭ１１０に与えられるプログラム用電源Ｖppの電圧は、一般的に、電源電圧Ｖccと同様とされている。また、ＳＩＭの内部でプログラム用電源Ｖppが発生されているものもある。ここでは、外部から供給する構造を示しているが、これは重要ではない。

【００２４】双方向データの入出力端子１０３は、双方向データ信号線Ｉ／Ｏにより実際にデータの入出力を行なうためのデータ入／出力端子である。双方向データ信号線Ｉ／Ｏには、シリアル／パラレル変換器１０７を介して、データが入／出力される。このデータ信号線Ｉ／Ｏは、入力或いは出力されていないときには、作動電源の電圧Ｖccと略同じ電圧に維持されており、外部の制御機器及びＳＩＭは、互いにデータ受信状態となっている。

【００２５】クロック入力端子１０４には、クロックＣＬＫが供給される。このクロックＣＬＫは、ＳＩＭに内蔵されているＣＰＵ（Central Processing Unit）１１２の作動用クロックである。また、このクロックＣＬＫは、分周器１０８で適当に分周されて、シリアル／パラレル変換器１０７に供給される。この分周器１０８で分周されたクロックＣＬＫは、双方向データ信号線Ｉ／Ｏで交換されるデータの転送速度を決める転送クロックとなる。

【００２６】リセット入力端子１０５には、リセット信号ＲＳＴが与えられる。このリセット信号ＲＳＴは、内蔵されているＣＰＵ１１２のみならず、分周器１０８や、シリアル／パラレル変換器１０７等を初期化するためにも用いられる。

【００２７】データの入／出力は、双方向データ信号線Ｉ／Ｏを介して、シリアル／パラレル変換器１０７により行なわれる。シリアル／パラレル変換器１０７は、外部機器からシリアルデータで転送されてきたデータを、例えば８ビットのパラレルデータに変換する。

【００２８】双方向データ信号線Ｉ／Ｏを介して入／出力されるシリアルデータは、「Ｌ」レベルのスタートビットが先頭にあり、その後ＬＳＢファーストの正論理（又はＭＳＢファーストの負論理、選択はＩＣカード製造業者が行う）でビットデータが続き、偶数のパリティ１ビットが付加される。「Ｌ」レベルのスタートビットによりデータの先頭が検出され、それに続いて、データが送られる。そして、パリティによりエラーが検出される。このとき、パリティによりエラーが検出されれば、パリティビットに続く２クロックの間の特定時間に、受信側から「Ｌ」レベルが送出される。これにより、送信側では、エラーがあったことが分かる。エラーがあったことを分かると、送信側は、同じデータを再度送信す

る。

【００２９】この方法は、ＩＳＯ７８１６の半二重非同期通信プロトコルである。シリアル／パラレル変換器１０７は、これらの処理を経て、シリアルデータとパラレルデータとの変換処理を行なう。

【００３０】ＲＡＭ（Random Access Memory）１０９は、随時書き込み読み出しが可能であり、このＲＡＭ１０９は、ＣＰＵ（Central Processing Unit）１１２が処理を行なっていく際に必要なデータを一時的に記憶したり、いくつかのデーター時的に蓄えておくために使用される。

【００３１】ＥＥＰＲＯＭ１１０は、内部だけで利用されるデータ、利用上更新しながら継続使用されるデータ等が記憶される。例えば、ディジタルセルラー携帯端末では、短縮ダイアル、契約内容、ショートメッセージ、或いは通信を開始、維持するための制御データ等がＥＥＰＲＯＭ１１０に記憶される。

【００３２】なお、ここでは、ＥＥＰＲＯＭを使用しているが、例えば、ＥＥＰＲＯＭの代わりに、フラッシュメモリを用いるようにしても良い。

【００３３】ＲＯＭ（Read Only Memory）１１１は、主に、ＣＰＵ１１２が処理すべきプログラムが記憶されている。処理命令は、例えば、携帯端末を製造したり、利用するのに必要な公開された命令体系と、セキュリティ、例えばスクランブルキー発生部や、発行者又は管理者利用できないデータなどを操作するための非公開の管理用命令体系や暗証番号からなる。このように、非公開の管理用命令体系を用意することで、ＳＩＭセキュリティ機能がさらに高められている。

【００３４】分周器１０８は、ＣＰＵ１１２を作動させるためのクロックＣＬＫから、双方向データ信号線Ｉ／Ｏ所定の伝送レートを使用してデータを送るためのクロックを得るものである。分周器１０８の分周比としては、例えば、ＧＳＭ方式の携帯電話システムでは、１／３７２が用いられている。勿論、この分周比は、使用目的や使用状況により変更し得るものである。

【００３５】ＣＰＵ１１２は、外部からの命令に従って、ＳＩＭ内部の処理を行うものである。この時、内部にアクセス権が或るか否か等が判断されて、処理が行なわれる。

【００３６】データ用バス１１３は、ＣＰＵ１１２が命令を実行する際に、命令をＲＯＭ１１１から読み出したり、一時的にデータを記憶させるために、ＲＡＭ１０９に随時読み出し／書き込みしたり、外部装置からの要求に基づいて、ＥＥＰＲＯＭ１１０をアクセスしたりする際に、データを転送するのに用いられる。

【００３７】このように、ＳＩＭの構成のＩＣカードでは、ＥＥＰＲＯＭ１１０には、短縮ダイアル、契約内容、ショートメッセージ、或いは通信を開始、維持するための制御データ等、内部だけで利用されるデータ、利用上更新しながら継続使用されるデータ等が記憶される。また、ＲＯＭ１１１には、例えば、携帯端末を製造したり、利用するのに必要な公開された命令体系と、セキュリティ、例えばスクランブルキー発生部や、発行者又は管理者利用できないデータなどを操作するための非公開の管理用命令体系からなる処理命令が記憶される。そして、入／出力されるデータは、ＣＰＵ１１２により管理されている。このため、高いセキュリティ機能が保証されている。

【００３８】２．メモリスティックの内部構成

次に、メモリスティックと呼ばれるメモリカードについて説明する。図２は、メモリスティックの内部構造を示すブロック図である。

【００３９】メモリスティックには、電源端子２０１と、外部機器との接続のためのデータ入／出力端子２０２と、バスステートの入力端子２０３と、シリアルクロックの入力端子２０４と、挿抜検出用の検出端子２０５と、接地端子２０６とが配設される。

【００４０】データ入／出力端子２０２により、双方向データ線ＤＩＯを介して、データが入／出力される。データ線ＤＩＯは、トランスファープロトコルコマンド（ＴＰＣ）という制御データやデータそのものを書き込んだり、読み出したりするためのものである。

【００４１】バスステートの入力端子２０３には、バスステートＢＳが供給される。バスステートＢＳは、双方向データ信号線ＤＩＯ上のデータに対するステータスを示している。例えば、データアクセスを行う前のＴＰＣやデータそのものにより、そのステートを変化させることにより、メモリスティックの処理が実行される。

【００４２】シリアルクロック端子２０４には、転送用クロックＳＣＬＫが供給される。転送クロックＳＣＬＫは、ＴＰＣやデータそのものを転送する際に発生される。転送クロックＳＣＬＫは、バスステートＢＳにより制御されている。

【００４３】検出端子２０５は、外部装置がメモリスティックの着脱状態を検出するために使用される。メモリスティック内部では、この検出端子２０５は接地されており、外部装置によりプルアップ抵抗を介して電源に接続されている。したがって、検出端子２０５は、メモリスティック装着状態では「Ｌ」レベルになり、非装着時には「Ｈ」レベルになる。

【００４４】接地端子２０６は、グランドＶssに接続されている。

【００４５】シリアル／パラレル変換器２０７は、書き込み時には、双方向データ信号ＤＩＯを通じ、転送クロックＳＣＬＫに同期して送られてきたシリアルデータを、８ビットのパラレルデータに変換する。制御用コマンドもデータも、ここでシリアルデータからパラレルデータに変換される。

【００４６】一方、読み出し時は、メモリスティック内

部のフラッシュメモリ２１３に記憶されている８ビット毎のパラレルデータは、シリアル／パラレル変換器２０７でシリアルデータに変換され、双方向データ信号ＤＩＯを通じて、外部装置に出力される。

【００４７】レジスタ２０８は、ステータスレジスタ、パラメータレジスタ、エキストラデータレジスタ等からなり、ＴＰＣによりメモリスティック内部のメモリのアクセス制御を行う。

【００４８】ページバッファ２０９は、シリアル／パラメータ変換器２０７とフラッシュメモリ２１３間でデータ交換を行う際、一時的にデータを記憶するのに用いられる。

【００４９】エラー検出コード発生部２１０は、例えば、ＣＲＣ（Cyclic Redundancy Check ）コード等のエラー検出コードを転送するデータ或いは転送されてくるデータに付加して、転送するデータ或いは転送されてくるデータの誤り検出を行なうものである。このようなエラー検出を行うことにより、データの信頼性が確保されている。

【００５０】アトリビュートＲＯＭ２１１は、メモリスティック内部の物理的情報を記憶するものである。このアトリビュートＲＯＭ２１１の情報は、電源オン直後に読み出される。外部装置は、この情報を対応状況をチェックするために用いる。

【００５１】フラッシュＩ／Ｆシーケンサ２１２は、レジスタ２０８に設定されているパラメータ等を基にして、ページバッファ２０９とフラッシュメモリ２１３間のデータの制御を行なっている。

【００５２】フラッシュメモリ２１３は、例えばＮＡＮＤ型のメモリセルからなる不揮発性のメモリカードを用いたもので、ある容量のページ単位に区切られて、データの書き込み／読み出しが行われる。このフラッシュメモリ２１３の記憶容量は多種あるが、例えば、６４ＭＢ程度まで計画されている。

【００５３】このように、メモリスティックでは、フラッシュメモリ２１３により、例えば、６４ＭＢ程度までのデータを記録できる。そして、このメモリスティックでは、シリアルの半二重同期データ転送方式を利用することで、２０Ｍｂ／秒程度のアクセス速度が確保できる。

【００５４】３．スマートスティックの一例

３－１．スマートスティックの一例の構成

この発明は、図２に示したメモリスティックの構成のメモリカードを基本構成として、図１に示したＳＩＭと呼ばれるＩＣカードとの互換性を各信号線ベースで維持できるようにして、メモリスティックをインテリジェント化したものである。このようにインテリジェント化されたメモリスティックは、通常のメモリスティックとして使用できると共に、ＳＩＭと呼ばれるＩＣカードと同様な機能を使うことができる。これにより、コンテンツのデータをダウンロードする際に、セキュリティが向上すると共に、電子マネー等により課金処理ができるようになる。以下、このようにインテリジェント化されたメモリスティックをスマートスティックと呼ぶことにする。

【００５５】図３は、この発明が適用されたスマートスティックの内部構造の一例を示すものである。図３に示すように、このスマートスティックには、電源端子３０１と、プログラム用電源端子３０２と、双方向データ信号線Ｉ／Ｏの入出力端子３０２と、バスステートの入力端子３０３と、転送クロック入力端子３０４と、挿抜検出用の検出端子３０６と、クロック入力端子３０６と、リセット入力端子３０７と、接地端子３０８が設けられる。

【００５６】電源端子３０１は、作動電源Ｖccを外部から供給するためのものである。作動電源Ｖccの電圧は５Ｖ～３Ｖである。

【００５７】入出力端子３０２は、双方向データ信号線Ｉ／Ｏにより実際にデータの入出力を行なうためのデータ入／出力端子である。双方向データ信号線Ｉ／Ｏには、ＳＩＭの双方向データ信号線（図１）又はメモリスティックの双方向データ信号線ＤＩＯ（図２）と同様である。

【００５８】バスステートの入力端子３０３には、バスステートＢＳが供給される。バスステートＢＳは、双方向データ信号線上でパケット通信でデータを転送する際、データに対するステータスを示している。例えば、データアクセスを行う前のＴＰＣやデータそのものにより、そのステートを変化させることにより、メモリスティックの処理が実行される。

【００５９】なお、データの入出力には、バスステートＢＳを使用しない非同期モードも可能である。この方式は、ＳＩＭで使用されているＩＳＯ７８１６の半二重非同期通信プロトコルである。

【００６０】転送クロック入力入力端子３０４には、転送用のシリアルクロックＳＣＬＫが供給される。この転送クロックＳＣＬＫは、パケット通信の状態で、バスステートＢＳによりクロック発生が制御される。半二重非同期通信プロトコルでは、転送クロックＳＣＬＫは使用されない。

【００６１】検出端子３０５は、外部装置がスマートスティックの着脱状態を検出するために使用される。スマートスティック内部では、この検出端子３０５は接地されており、外部装置によりプルアップ抵抗を介して電源に接続されている。したがって、検出端子３０５は、メモリスティック装着状態では「Ｌ」レベルになり、非装着時には「Ｈ」レベルになる。

【００６２】クロック入力入力端子３０６には、作動クロックＣＬＫが供給される。この作動クロックは、ＣＰＵ３０６を作動させるために、ＣＰＵ３１６に供給される。

【００６３】リセット入力端子３０７には、リセット信号ＲＳＴが供給される。このリセット信号ＲＳＴにより、内蔵されているＣＰＵ３１６が初期化されると共に、シリアル／パラレル変換器３０９や、制御用のレジスタ３１０、スクランブラ３１１ａ等が初期化される。

【００６４】接地端子３０８は、グランドVssに接続されている。

【００６５】シリアル／パラレル変換器３０９は、外部装置とのデータの交換を行なえるように、シリアルデータとパラレルデータとの変換を行なっている。外部装置との間では、双方向データ通信線Ｉ／Ｏを介して、シリアルデータで転送が行なわれ、内部では、８ビットのパラレルデータで処理が行われる。シリアル／パラレル変換器３０９は、シリアルデータと、８ビットのパラレルデータとの変換処理を行なっている。

【００６６】レジスタ３１０は、ステータスレジスタとコントロルレジスタからなり、ＣＰＵ３１６がシリアル／パラメータ変換器３０９の監視と制御を行なうために用いられる。

【００６７】スクランブラ３１１ａは、データを暗号化して記憶させることができるようにするものである。暗号化してデータを記憶させるのは、記憶されているデータの保護を図るためである。例えば、何かの方法でフラッシュメモリ３１５の部分だけを取り外すことができたとすると、悪意のある試みとして、何人かにより、フラッシュメモリ３１５の部分だけが取り出され、フラッシュメモリ３１５の内容が読み取られ、そこに書かれているコンテンツや個人情報が盗まれる危険性がある。フラッシュメモリ３１５にデータを記憶させる際に、データを暗号化しておけば、たとえフラッシュメモリ３１５の部分だけが取り出され、その内容が読み取られたとしても、コンテンツや個人情報については保護できる。スクランブラ３１１ａの暗号化のアルゴリズムについては、後に、詳述する。

【００６８】エラー検出コード発生部３１１ｂは、例えば、ＣＲＣ（Cyclic Redundancy Check）コード等のエラー検出コードを転送するデータ或いは転送されてくるデータに付加して、転送するデータ或いは転送されてくるデータの誤り検出を行なうものである。このようなエラー検出を行うことにより、データの信頼性が確保されている。

【００６９】ページバッファ３１２は、予め決められたデータ容量を一時的に記憶し、シリアル／パラメータ変換器３０９とフラッシュメモリ３１５間でデータ交換を行う際、一時的にデータを記憶するのに用いられる。

【００７０】ＲＡＭ３１３は、ＣＰＵ３１６が外部装置から与えられた命令を処理する際に、一時的に発生する演算結果、パラメータ等を記憶するために用いられる。

【００７１】ＲＯＭ３１４は、主に、ＣＰＵ３１６が処理すべきプログラムが記憶されている。処理命令は、例えば、携帯端末を製造したり、利用するのに必要な公開された命令体系と、セキュリティ、例えばスクランブルキー発生部や、発行者又は管理者以外は利用できないデータなどを操作するための非公開の管理用命令体系や暗証番号からなる。このように、非公開の管理用命令体系を用意することで、セキュリティ機能がさらに高められている。

【００７２】また、ＲＯＭ３１４には、外部から見えるファイルと、管理用及び暗号に関係した処理にのみ使用される管理用命令体系以外ではアクセスできない隠されたファイル等を操作するためのプログラムが記憶されている。

【００７３】フラッシュメモリ３１５は、例えばＮＡＮＤ型のメモリセルからなる不揮発性のメモリカードを用いたものである。メモリフラッシュメモリ３１５には、見えるファイルも管理用の外部から見えないファイルも、後に説明するディレクトリデスクリプションやファイルデスクリプションに従って、フラッシュメモリ３１５に記憶される。

【００７４】ＣＰＵ３１６は、外部装置から転送された命令を、読み出し専用メモリ３１４から必要なプログラムを随時読み出して処理を行う。

【００７５】３－２．外部装置とスマートスティックとのセッション

次に、外部装置であるホストコンピュータが、上述のようにインテリジェント化されたメモリスティック（スマートスティック）をどのように制御するかについて説明する。

【００７６】図４は、外部装置が上述のスマートスティックを制御する際のセッションを示すもので、これは、従来のＧＳＭ方式の携帯電話におけるＳＩＭの制御を行なうのに適用したものである。

【００７７】先ず、スマートスティックを起動するために、ホストコンピュータは、電源Vcc、クロックＣＬＫ、リセット信号ＲＳＴの供給を行なう（ステップＳＴ１）。送る順番は、電源電圧Vcc、プログラム電源Vpp（内部で供給する場合には不要、また外部から供給する場合ＶＣＣと同時であっても良い）、クロックＣＬＫ、リセット信号ＲＳＴの順である。

【００７８】リセット信号ＲＳＴを「Ｌ」レベルから「Ｈ」レベルに状態変化させると、スマートスティックは動作状態に入る（ステップＳＴ２）。スマートスティックの内部では、ホストコンピュータから命令を受け取るための初期化が行なわれる。

【００７９】次に、ホストコンピュータはスマートスティックに、実行命令コマンドを送る（ステップＳＴ３）。この実行命令コマンドは、例えばいくつかのバイトで構成されており、最初のバイトは応用分野毎にコードが予め決められている。このことにより、マルチファンクションの動作が可能になる。次のバイトは処理命令

コードを表し、それに続くバイトは命令を実行する際に必要なパラメータなどからなる。

【００８０】スマートスティックは、ホストコンピュータから実行命令コマンドを受け取り、そのコマンドを確認できると、ホストコンピュータにアクノリッジを返す（ステップＳＴ４）。

【００８１】次に、ホストコンピュータがコマンドを送り、スマートスティックからアクノリッジが返されると、ホストコンピュータとスマートスティックとの間でデータのやり取りが可能となる。そして、実行命令コマンドの内容に従って、ホストコンピュータからスマートスティックに向かって、或いはスマートスティックからホストコンピュータに向かって、データが転送される（ステップＳＴ５）。

【００８２】最後に、スマートスティックは、実行命令終了状況をホストコンピュータへ知らせるために、２バイトのステータワードをホストコンピュータに送出する（ステップＳＴ６）。

【００８３】その後の通常のセッションでは、ホストコンピュータからスマートスティックへの実行命令コマンドの送出（ステップＳＴ３）から、スマートスティックからホストコンピュータへのステータスワードの送出（ステップＳＴ６）までが１回のアクセスとして、セッションが繰り返される。

【００８４】３－３．暗号化について

図３に示したように、この発明が適用されたスマートスティックでは、フラッシュメモリ３１５に、データを暗号化して記憶させることができる。このときの暗号化キー生成について説明する。

【００８５】図５は、暗号化キーの生成処理を示すものである。図５において、暗号化キー演算回路４０３は、２つのパラメータから暗号化キーを発生するアルゴリズムの演算を行なうものである。暗号化キー演算回路４０３は、図３におけるスクランブラ３１１ａにハードウェアとして設けられる。

【００８６】暗号化キー演算回路４０３には、入力端子４０１及び４０２から２つのパラメータが与えられる。一方のパラメータとしては、ユーザの暗証番号（ＰＩＮ：Personal ID Number）が使用される。なお、この暗号化キー生成用のパラメータとしては、暗証番号でなくてもよく、例えば、カード発行時に会社に登録されている加入者番号や、ある特定グループ内で使用されるコードであっても良い。

【００８７】他方のパラメータとしては、暗号情報Ｋｉが用いられる。前述したように、スマートスティックの命令体系には、公開されている命令体系と、非公開の命令体系とがあり、非公開の命令体系は、発行者又は管理者以外利用できない。暗号情報Ｋｉは、非公開の命令体を使わないとアクセスできないように設定されている。

【００８８】暗号化キー演算回路４０３で、ユーザのＰＩＮと暗号情報Ｋｉをパラメータとして、暗号化キーが生成される。そして、暗号化キー演算回路４０３により生成された暗号化キーＫｃが出力端子４０４から出力される。

【００８９】上述のようにして生成された暗号化キーＫｃを使用して、図６に示すような暗号化処理回路により、暗号化処理が行なわれる。

【００９０】図６において、暗号化アルゴリズム演算回路４５２は、所定の暗号化アルゴリズムにより、入力データを暗号化して出力するものである。暗号化アルゴリズム演算回路４５２は、図３におけるスクランブラ３１１ａにハードウェアで構成されている。

【００９１】暗号化アルゴリズム演算回路４５２には、入力端子４５１から暗号化キーＫｄが供給される。この暗号化キーＫｄは、図５の暗号化生成例で示した演算結果として得られた暗号化キーＫｃに、変化するパラメータ（ここでは、ページモードアクセスする際のページ番号）を加えた値である。

【００９２】このように、生成された暗号化キーＫｃにある基準からの相対番号を加えた値を暗号化キーとしているのは、セキュリティを強化するためである。暗号化キーＫｃが変化しない場合には、暗号化されたデータと平文とを比較によりスクランブルアルゴリズムを予測して暗号を解読するという可能性が残され、セキュリティ上問題となる可能性がある。

【００９３】なお、ここでは、暗号化キーＫｃに対して変化するパラメータとしてページモードアクセスする際のページ番号を用いているが、この変化するパラメータは、入出力時に一致するものであれば何でも良く、例えば、電子的書き換え可能な不揮発性メモリ、フラッシュメモリのデータが格納される最初のアドレスを基準にした相対値でも良い。

【００９４】暗号化アルゴリズム演算回路４５２には、入力端子４５３から、平文のデータ（暗号化前のデータ）が与えられる。この平文のデータは、外部装置からシリアルデータとしてて送られてきた後、シリアル／パラレル変換器３０９で８ビット変換されたデータを意味している。暗号化アルゴリズム演算回路４５２で、この入力データに対して、入力端子４５１からの暗号化キーＫｄ（暗号化キーＫｃ＋ページ番号）を用いて、暗号化が行なわれる。

【００９５】暗号化アルゴリズム演算回路４５２により暗号化されたデータが出力端子４５４から出力される。この暗号化されたデータがフラッシュメモリ３１５（図３）に記憶される。

【００９６】このように、スクランブラ３１１ａ（図３）にハードウェアで構成された暗号化アルゴリズム演算回路４５２には、平文のデータと、暗号化キー（暗号化キーＫｃ＋ページ番号）とが供給され、暗号化アルゴリズム演算回路４５２により、所定の暗号化アルゴリズ

ムにより、暗号化データが生成される。この暗号化されたデータが出力端子４５４から出力され、最終的に、フラッシュメモリ３１５（図３）に記憶される。

【００９７】なお、上述の例では、外部装置から入力された平文のデータを暗号化してフラッシュメモリ３１５に記憶させる際の処理について説明したが、フラッシュメモリ３１５に記憶されているデータを読み出し、暗号化されたデータを解読して平文のデータに戻して、外部装置に出力する際の処理については、上述の手順と逆の手順で行なえば良い。

【００９８】また、フラッシュメモリ３１５にデータを記憶させる場合に、常に、データを暗号化する必要はない。必要に応じて、データを暗号化せず、平文データのままフラッシュメモリ３１５に記憶させ、フラッシュメモリ３１５から平文で出力させることも可能である。また、これとは反対に、フラッシュメモリ３１５にデータを暗号化して記憶させ、この暗号化されたデータが記憶されているフラッシュメモリ３１５から、暗号解読しないまま、暗号化されたデータを外部装置に出力することも可能である。

【００９９】３－４．ファイル構成について

次に、フラッシュメモリ３１５上に展開されるデレクトリやファイルの構成について説明する。このファイル展開の方式は、ＧＳＭ方式の携帯電話で使用されているＳＩＭのファイル管理方式に改良を加えたものである。

【０１００】図７は、ディレクトリの仕様を示すものである。ディレクトリのデスクリプションは、メインディレクトリと、メインディレクトリの下に構成されるサブディレクトリの情報を提供するものである。メインディレクトリのデスクリプションと、サブディレクトリのディスクリプションは同様である。

【０１０１】この発明が適用されたスマートスティックをマルチファンクションで使用する場合、例えば、通信用のメインディレクトリ、電子出版用のメインディレクトリ、ゲームのダウンロード用のメインディレクトリ、或いは最終使用者が自由に利用できるディレクトリ等に分けて使用することが想定される。このような場合、それぞれの目的に応じてセキュリティの設定条件が異なるため、それぞれで管理情報を有することになる。

【０１０２】図７は、ディレクトリのデスクリプションを示すものである。ディレクトリのデスクリプションは、メインディレクトリ又はサブディレクトリの容量、ファイル数、セキュリティ用の暗証番号機能が提供されているか、クロック停止が可能かどうか等の情報が含まれている。管理用の隠されたディレクトリ以外は、この情報は外部装置から読み出すことが可能で、メモリスティックを制御するためにも使用される。

【０１０３】ディレクトリのデスクリプションは、共通の仕様（図７Ａ）と、各アプリケーション用の仕様（図７Ｂ）に大別される。

【０１０４】先ず、図７Ａに示す共通の仕様について説明する。共通仕様では、アプリケーションによらず、全てに共通したフォーマットでコーディングされる。共通仕様のバイトＢ１～バイトＢ４は、残存有効メモリ量を示しており、スマートスティック全体で利用できる残りのメモリ量を示す。

【０１０５】バイトＢ５～バイトＢ２０は、ディレクトリＩＤ及びタグで、２バイトのコードと残りは例えばＡＳＣＩＩの平文タイトルなどに使用される。ディレクトリＩＤ及びタグは、ここでは例として１６バイトを設定しているが、勿論、より多くのバイト数を割り当ててもかまわない。

【０１０６】バイトＢ２１はディレクトリタイプで、ディレクトリ或いはファイルの識別をするためのデータをコーディングしている。図７Ｃは、バイトＢ２１のコーディング例を示している。例えば、マルチファンクションで使用する場合、アプリケーション毎のメインディレクトリは「０１ｈ（ｈは１６進数を示す）」、その下のサブディレクトリは「０２ｈ」、データファイルを表す場合は「０４ｈ」にコーディングされる。

【０１０７】バイトＢ２２～バイトＢ２７はタイムスタンプである。このタイムスタンプは、ＧＳＭ方式の携帯電話におけるＳＩＭには用いられていない情報である。例えばフロッピーディスクやハードディスク等で新たにディレクトリを作成した場合には、必ずタイムスタンプが規約される。このタイムスタンプは、そのことを想定して設けたものである。また、発行者が時限付きで使用を許諾するようなソフトウェアの販売や電子出版にも、タイムスタンプは使用可能である。例えば、タイムスタンプを参考にして期限切り換えられると、内容を読み出させないするという操作も可能である。ここでは、時刻分単位までの記入例だが、勿論、秒単位であっても良い。

【０１０８】バイトＢ２８～Ｂ２９は、将来の拡張性を鑑みて、リザーブされている。

【０１０９】バイトＢ３０は、次に続くアプリケーション用のファイルのデータ長で、各アプリケーション用の仕様のサイズで、どこまでがディレクトリデスクリプションかを示すために用いられる。サブディレクトリデスクリプションやデータファイルがこれに連続してアプリケーション可能なようにし、メモリの有効活用をする。

【０１１０】次に、図７Ｂに示す各アプリケーション毎の仕様について説明する。図７Ｂにおいて、バイトＢ３１はディレクトリキャラクタリスティクスである。図７ＤがそのコーディングＣＰＵ用の作動クロックの停止が可能か否か、停止可能な場合の状態が「Ｈ」レベル或いは「Ｌ」レベルで、停止するのかどちらでも良いのかがコーディングされている。また、停止したときの状態により消費電流が変わる場合もあり、携

帯端末等では少しでもこれを少なくできるように配慮している。

【0111】また、ディレクトリキャラクタリスティクスのビットBit8は、PIN1が有効であるか無効であるかを示している。PIN1は、主に使用者の正当性を確認するための暗証番号が設定されており、この状態が簡単にチェックできる。

【0112】バイトB32～バイトB33は、サブディレクトリ数を示し、例えば、マルチファンクションで使用されている場合に、アプリケーション別に設定されるメインディレクトリの下に、サブディレクトリがいくつ存在しているかをコーディングしている。

【0113】バイトB34～バイトB35は、ファイル数を示し、例えば、マルチファンクションで使用されてる場合に、アプリケーション別に設定されるメインディレクトリの下とサブディレクトリの下に、ファイルがいくつ存在しているかをコーディングスしている。

【0114】バイトB36は、PIN、アンブロックキングPIN、アドミニストレイティブコード数で、暗証番号、暗証番号がブロックされている場合の解除番号、或いは管理用の特別なコードがいくつ設定されているかを示している。例えば、PINが2種類設定されており、更に一般的には公開されず利用できない管理者用のアドミニストレーティブコードが2種類設定されていたとすると、「4（h）」という値にコーディングされる。

【0115】バイトB37は、将来の拡張性のためにリザーブされている。

【0116】バイトB38は、PIN1ステータスである。図7Eに、セキュリティステータスのコーディングが示されている。例えば、PIN1が設定されていたなら、ビットBit8が「1」にコーディングされ、更に、連続誤入力カウンタが「3」に設定されていたなら「83（h）」というコードになる。この場合、連続してPIN1の暗証番号を誤ると、PIN誤入力カウンタは「0」になり、使用者はこれ以上PIN1の検証をすることがでくなくなる。この状態をPIN1がブロックされているという。また、PIN1の検証が正しく行なわれた場合は、PIN誤入力カウンタの値は初期値「3」にリセットされる。

【0117】バイトB39は、アンブロッキングPIN1ステータスを示している。図7Eに、セキュリティステータスのコーディングが示されている。例えば、PIN1が設定されていたなら、それと一対をなすこのアンブロッキングPIN1ステースのビットBit8が「1」にコーディングされる。PIN1ステータスの誤入力カウンタが「0」で、PIN1がブロックされた場合に、これを解除するために別に用意された暗証番号PUK（Unblocking Personal Key）であり、この状態を示しているのが、アンブロッキングPIN1ステータスである。

【0118】このアンブロッキングPIN1ステータスも、例えば、連続誤入力カウンタが「10」に設定されていたなら、「8A（h）」というコードとなる。この場合、連続して10回この暗証番号PUK1を誤ると、アンブロッキングPIN1誤入力カウンタは「0」になり、使用者はこれ以上PIN1のブロック解除を行うための暗証番号PUK1の検証ができなくなる。この状態では、最早、発行者或いは管理者が使用する管理命令体系を使用して復元するしか手段がなくなる。このような点も、セキュリティを高めている。また、PIN1ブロック解除用の暗証番号PUK1の検証が正しく行なわれた場合は、PUK1誤入力カウンタの値は初期値「10」にリセットされ、使用者は新たにPIN1を設定する。

【0119】バイトB40はPIN2ステータス、バイトB41はアンブロッキングPIN2ステータスを示している。PIN2ステータス、アンブロッキングPIN2ステータスは、PIN1ステータス及びアンブロッキングPIN1ステータスと同様である。

【0120】バイトB42～B48はアドミニストレーティブマネージメントユーズで、例えば、端末製造業者等には公開されていない命令体系を使用する場合に利用される。

【0121】次に、データファイルのアクティブ等を直接管理するための情報が記述しているファイルデスクリプションについて説明する。

【0122】図8は、ファイルデスクリプションを示すものである。このファイルデスクリプションは、共通仕様（図8A）と、各アプリケーション用の仕様（図8B）とに分けることができる。

【0123】図8Aは、共通仕様を示している。図8Aにおいて、バイトB1～バイトB4は、ファイルサイズを示している。

【0124】バイトB5～バイトB20は、ファイルID及びタグで、2バイトのコードと残りは例えばASCIIの平文タイトルなどに使用する。ファイルID及びタグは、ここでは例として16バイトを設定しているが、勿論もっと多く割り当ててもかまわない。

【0125】バイトB21はファイルタイプである。図8Cはコーディング例を示している。データファイルの場合には、「04（h）」にコーディングされる。

【0126】バイトB22～バイトB27はタイムスタンプで、GSM方式の携帯電話におけるSIMにはない情報である。例えばフロッピー（登録商標）ディスクやハードディスク等で新たにディレクトリを作成した場合には、必ずタイムスタンプが規約される。このタイムスタンプは、そのことを想定して設けたものである。また、発行者が時限付きで使用を許諾するようなソフトウェアの販売や電子出版にも、タイムスタンプは使用可能

である。例えば、タイムスタンプを参考にして期限切り換えられると、内容を読み出させないするという操作も可能である。ここでは、時刻分単位までの記入例だが、勿論、秒単位であっても良い。

【０１２７】バイトＢ２８はモードを示している。図８Ｄはそのコーディング例を示す。例えば、課金情報などの単位を一定時間毎に１命令でインクリンメト可能なファイル構造を有するファイルで、この命令が実行可能か否かを示している。例えば、課金情報がもうインクリンメトできない状態までカウントアップされたら、このスマートスティックが利用できないなどの管理に利用できる。

【０１２８】バイトＢ２９～バイトＢ３２はアクセスコンディションを示ししている。図８Ｅはそのコーディング例を示す。各バイト毎に対応した命令を実行するときに、満たされている必要のあるセキュリティ条件を設定する。

【０１２９】ここでバイトＢ３２は、スマートスティックのアクセス条件を示している。図８Ｆはコーディング例である。バイトＢ３２のビットＢｉｔ１～Ｂｉｔ４は、スクランブルを使用する際に、また、ビットＢｉｔ５～ビットＢｉｔ８は、コピーに関連してたアクセスをする際に、満たさなければならない条件で、そのコーディングがアクセスコンディションで示される。

【０１３０】アクセスコンディションコードが「０（ｈ）」のときには、常にアクセス可能である。「１（ｈ）」のときには、ＰＩＮ１の検証が正常に終了していた場合にアクセスが可能である。「２（ｈ）」のときには、ＰＩＮ２の検証が正常に終了した場合にアクセスが可能である。「３（ｈ）」は、将来の拡張のためにリザーブされている。「４（ｈ）は非公開の管理用のアクセス条件を満たしたときに利用できることを意味している。Ｆ（ｈ）はアクセスが不可能であることを示している。例えば、バイトＢ３２が「０１（ｈ）」とコーディングされていたら、スクランブルはＰＩＮ１の検証が正常終了した場合には利用でき、コピーは自由に可能であることを示している。

【０１３１】バイトＢ３３はファイルステータスであり、このファイルの状態を示している。図８Ｇはコーディング例である。例えば、ビットＢｉｔ１はこのファイルが利用できるか否かを示す。また、ビットＢｉｔ２は記録されているデータがスクランブルされているか否かを示す。

【０１３２】バイトＢ３４は、次に続くアプリケーション用のファイルデータ長で、各アプリケーション用の仕様のサイズで、どこまでがディレクトリデスクリプションかを示すために用いられる。サブディレクトリデスクリプションやデータファイルがこれに連続して位置できるようにして、メモリの有効活用がなされる。

【０１３３】次に、各アプリケーション用の仕様の内容について説明する。図８Ｂは各アプリケーション用の仕様を示すものである。図８Ｂにおいて、バイトＢ３５はストラクチャオブデータファイルで、ファイルの論理構造を示している。

【０１３４】ストラクチャオブデータファイルが「００（ｈ）」にコーディングされた場合には、通常のメモリと同じように、ある容量のデータがそのまま記憶される。「０１（ｈ）」にコーディングされた場合には、ある決まったフォーマットのデータがグループ化されて記録されていく。例えば、短縮ダイアルの１件分を５０バイトとした場合、この１件分をレコードと称してまとめて扱い、例えば、１００レコードとして５ｋバイトのメモリが確保されることになる。「０３（ｈ）」にコーディングされた場合は、「０２（ｈ）」のリニアフィックスと同レコードのフォーマットを有するが、このレコードの順番を順次入れ換えることができる。これは、優先順位を変更して、例えば、最初のレコードに持ってくるというような利用が可能である。つまり、受信に第１レコード、第２レコードから始まり、第ｎレコードまでとすると、このレコードの順番を入れ替え、第１レコードを第ｎレコードにし、それまで第２レコードであったレコードを新たに第１レコードとする方法である。

【０１３５】バイトＢ３６～バイトＢ３７は、レングスオブレコードで、１つのレコードのメモリサイズを示している。ファイルサイズとこのレングオブレコードから、いくつのレコードが使用できるか算出が可能である。

【０１３６】３－５．アクセス処理について

以下、この発明が適用されたスマートスティックのアクセス処理について、いくつかの命令処理を例にとって、フローチャートを使用して説明する。

【０１３７】図９は、この発明が適用されたスマートスティックの基本的動作を示している。図９において、パワーオンで、外部装置から電源を供給する。この時、必要ならば、フラッシュメモリのプログラ電源Ｖppを同時に供給する（ステップＳ１１）。

【０１３８】次に、ＣＰＵ作動クロックの供給ＣＬＫを外部装置から供給する（ステップＳ１２）。その後、リセット信号が「Ｌ」レベルから「Ｈ」レベルに変化して、ＣＰＵが作動状態に入るか否かの判断を行なう（ステップＳ１３）。

【０１３９】外部装置がスマートスティックを起動させていない場合には、リセット信号は「Ｌ」レベルから「Ｈ」レベルに変化しない。このときには、パワーオフ判断（ステップＳ２０）に進む。

【０１４０】一方、外部装置がスマートスティックを起動した場合には、リセット信号は「Ｌ」レベルから「Ｈ」レベルに変化する。このときには、初期化設定に移り（ステップＳ１４）、外部装置からのコマンド受領、データ交換の準備をする。

【0141】次に、外部装置からコマンド待ち状態で、コマンドが入力されるか否かが判断される（ステップS15）。もし、コマンドの入力がなければ、リセット信号RSTのチェックに移る（ステップS19）。

【0142】一方、ステップS15で、コマンド入力があったら、そのコマンドを受付たことを外部装置に回答するために、アクノリッジの出力処理を行なう（ステップS16）。続いて、そのコマンドに対応処理として、データの出力処理又は入力処理のデータ処理を行なう（ステップS17）。そして、その処理の終了状況を外部装置に知られるために、ステータスワードを出力する（ステップS18）。

【0143】これが終了したら、リセット信号をチェックするために、リセット信号判断を行ない（ステップS19）、リセット信号RSTが「H」レベルなら、再びコマンドを受け付けるために、パワーオフ判断を行う（ステップS20）。

【0144】ここで、パワーオフであければ、リセットチェックに戻り（ステップS13）、パワーオフであれば全ての機能を停止する処理に移り、処理を完了する（ステップS21）。

【0145】次に、セキュリティに関係した暗証番号の処理について、図10のフローチャートを参照して説明する。

【0146】なお、ディレクトリデスクリプションで記述したPIN1、PIN2、PUK1、PUK2の扱いは、誤り入力数が異なるだけで処理についてはと同様であるから、一括して説明する。

【0147】図10において、PIN入力があったときに、スタートS31から処理を開始する。

【0148】次に、PIN1、PIN2、PUK1、PUK2の何れかを設定するPINモードの設定を行う（ステップS32）。この設定に従って、該当するPINが初期化されているか否かの判断を行なう（ステップS33）。

【0149】初期化されていない場合には、初期化されていないことを示すステータスを、図9メインルーチンフローチャートの中のステータスワードアウトプット処理（ステップ18）にて、外部装置に出力し（ステップS40）、処理を終了する（ステップS45）。

【0150】初期化されていたなら、PINがブロックされているか否かをチェックするために、誤入力カウンタの値が「0」か否かを判断する。もし、誤入力カウンタが「0」であったならば、外部装置にブロックされていることを示すステータスを出力する（ステップS44）。

【0151】誤入力カウンタが「0」でなかったならば、該当するPINがブロックされていないので、次に、該当するPINの検証機能が必要かのPINイネーブル判断処理がなされる（ステップS35）。該当するPINの検証機能が不要に設定されている場合には、PINがディスイネーブルであることを示すステータスを外部装置に出力する（ステップS41）。

【0152】PINの検証機能が必要な場合には、予め記憶してある該当PINの内容と、入力されたPINの比較を行なう（ステップS36）。

【0153】この結果、予め記憶されているPINと、入力されたPINとが一致したか否かを判断する（ステップS37）。もし、入力されたPINが誤りならば、誤入力カウンタを更新するための誤入力カウンタのデクリメント処理を行い（ステップS42）、更に誤ったPINの入力があったことを外部装置に知らせるために、PINが誤っていることを示すステータスを出力して（ステップS43）、処理を終了する（ステップS45）。

【0154】予め記憶してあるPINと入力されたPINが一致した場合には、誤入力カウンタを初期化し、それに加えて関連するPINの誤入力カウンタも同時に初期化可する（ステップS38）。そして、通常終了コマンドを示すステータスを出力して（ステップS39）、処理を終了する（ステップS45）。

【0155】次に、ファイルアクセスの処理について、ファイル更新処理を例にして説明する。なお、他のコマンドの処理も同様に行なわれる。

【0156】図11は、ファイル更新のフローチャートを示すものである。まず、外部装置から更新コマンドが入力され、処理が起動される（ステップS51）。

【0157】次に、ファイルデスクリプション（図8）中で、更新の条件がコーディングされているバイトB29のビットBit1～Bit4（図8F参照）を参照するために、更新条件の設定をCPUが行う（ステップS52）。次に、ファイルデスクリプション中のアクセスコンディションコードのどれに該当するかを順次チェックする。

【0158】最初にファイルのアクセスが禁止されているか否かの判断を行なう（ステップS53）。もし、アクセスが禁止されているならば、外部装置に条件が不十分である旨を通知するアクセス条件が満足しないことを示すステータスを出力する（ステップS69）。

【0159】ステップS53で、もし、アクセスが禁止されていなければ、管理上のコード検証に該当するか否かを判断する（ステップS54）。もし、該当するなら、検証判断（ステップS57）に進む。

【0160】もし、管理上のコードに該当しないならば、PIN1での検証に該当するか否かを判断する（ステップS55）。該当するなら、検証判断（ステップS57）へ進む。

【0161】該当しない場合は、図8に示したファイルデスクリプション中のアクセスコンディションコードの検証不要コード（ALW）に該当するので、ステップS

５８に進み、スクランブル条件の判断設定を行なう。

【０１６２】ステップＳ５４、ステップＳ５５及びステップＳ５６での判断の結果、いずれかに該当すると判断された場合には、該当するＰＩＮ或いはコードの検証が済んでいるか否かの判断を行なう（ステップＳ５７）。

【０１６３】該当するＰＩＮ或いはコードの検証が済んでいない場合は、外部装置にＰＩＮの検証が済んでいないことを示すステータスを出力する（ステップＳ６８）。

【０１６４】次に、図８に示したファイルデスクリプション中のアクセスコンディションコードのどれに該当するかを順次チェックする。

【０１６５】最初に、管理上のコード検証に該当するか否かを判断する（ステップＳ５９）。もし、管理上のコードに該当しなければ、ＰＩＮ１での検証に該当かを判断する（ステップＳ６０）。ＰＩＮ１での検証に該当しないなら、ＰＩＮ２での検証に該当するかを判断する（ステップＳ６１）。該当しない場合には、ファイルデスクリプション中のアクセスコンディションの不使用コード（ＮＥＶ）に該当するので、スクランブルを使用しない設定をして処理を行う（ステップＳ６７）。

【０１６６】一方、ステップＳ５９、Ｓ６０、Ｓ６１の何れかで、条件に該当すると判断された場合には、該当するＰＩＮ或いはコードの検証が済んでいるか否かの判断を行う（ステップＳ６２）。該当するＰＩＮ或いはコードの検証が済んでいない場合には、外部装置に、ＰＩＮの検証は不成功であることを示すステータスを出力する（ステップＳ６８）。

【０１６７】ステップＳ６２で、検証が済んでいると判断された場合には、暗号化キーＫｃを参照するために、暗号化キーの計算処理を実行する（ステップＳ６３）。ここで得られた暗号化キーＫｃを使って、暗号キー（Ｋｃ＋ページ番号）により暗号化するような、スクランブルモードとなるように、スクランブラモードに設定する（ステップＳ６４）。このとき、例えば、複合暗号キーの一部をなすページ番号は、ハードウェアから直接入力してもかまわない。

【０１６８】こうして、事前にスクランブルを使用するか否かを選択された後、実際にデータの更新が実行され（ステップＳ６５）、全てのデータの更新が完了した時点で、外部装置に正常終了を知らせるステータスを出力して（ステップＳ６６）、終了となる（ステップＳ７０）。

【０１６９】４．スマートスティックの他の例

次に、この発明が適用されたスマートスティックの他の例について説明する。図１２は、この発明が適用されたスマートスティックの他の例の内部構造を示すものである。

【０１７０】前述の図３に示したスマートスティックでは、シリアル／パラレル変換器３０９に対する転送用クロックＳＣＬＫをクロック入力端子３０４から供給するようにしているが、この例では、ＣＰＵの作動クロックを分周器３２０で分周して、転送用のクロックＳＣＬＫとしている。その他の構成については、前述の図３に示した例と同様である。

【０１７１】このように、転送クロックＳＣＬＫを作動クロックＣＬＫを分周して形成することにより、クロックに係わる信号線が１つ不要になり、単一クロックでの動作が可能となる。これにより、外部装置の負担が軽減される。

【０１７２】一方、この例では、転送クロックＳＣＬＫは作動クロックＣＬＫの関係が分周器３２０の分周比で決められるため、転送クロックＳＣＬＫ及び作動クロックＣＬＫの周波数を任意に決められなくなる。また、転送クロックＳＣＬＫと作動クロックＣＬＫとを独立して止められなくなる。

【０１７３】このことは、とりもなおさず、ＩＳＯ７８１６に規定されている半二重非同期通信プロトコルに対応した動作で、特に、負の要因とはならない。むしろ、ＧＳＭ等で仕様されているＳＩＭの代替えとしての可能性が増すことになる。

【０１７４】また、この例では、ＣＰＵが処理を行なっていない場合、適正な手順で作動クロックを停止させることができる。この作動クロック或いは転送クロックの停止機能は、携帯端末において、バッテリ駆動されるという観点から、消費電力の低減が必須となり、有効な手段と言える。

【０１７５】なお、この発明が適用されたスマートスティックは、ＣＰＵを内蔵しているため、コンテンツデータの記憶用としてばかりでなく、種々の分野に応用可能である。例えば、外部記憶ばかりでなく、パーソナルコンピュータのコプロセッサとしても利用できる。

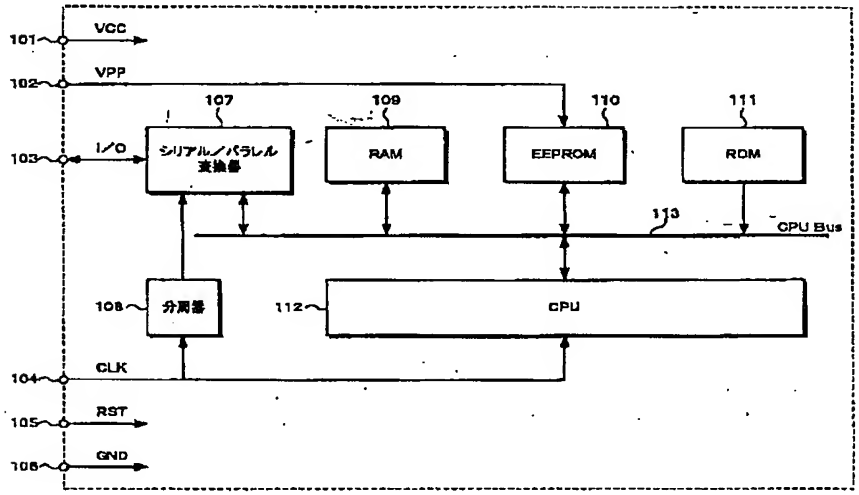
【０１７６】

【発明の効果】この発明によれば、メモリスティックの構成のメモリカードに、ＣＰＵと、暗号化回路が設けられる。そして、入出力されるデータは、暗号化されて、フラッシュメモリに記憶される。また、メモリスティックをアクセスするための命令体系には、公開された命令体系と非公開の命令体系とを有している。フラッシュメモリに記憶されるファイルデータは、各ファイルデータ毎に、アクセス制限、コピーガード情報、及びアクセス時の暗号化、暗証番号を選択的に設定できる。これらのファイルデータは、隠されたデータファイルを含むデータファイルが処理を管理している。また、ファイルデータにはアクセス権が設定され、アクセス権に従って、ファイルデータの読み出し及び書き込みのアクセスが制限される。このように、データが暗号化されてフラッシュメモリに記憶されるため、記憶されるデータのセキュリティが強化される。

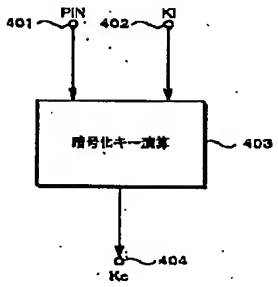
【図面の簡単な説明】

【図１】ＳＩＭの説明に用いるブロック図である。
【図２】メモリスティックの説明に用いるブロック図である。
【図３】この発明が適用されたメモリカードの一例のブロック図である。
【図４】この発明が適用されたメモリカードの一例の説明に用いる略線図である。
【図５】この発明が適用されたメモリカードの一例における暗号化の説明に用いるブロック図である。
【図６】この発明が適用されたメモリカードの一例における暗号化の説明に用いるブロック図である。
【図７】この発明が適用されたメモリカードの一例におけるディレクトリの説明に用いる略線図である。
【図８】この発明が適用されたメモリカードの一例におけるファイルの説明に用いる略線図である。
【図９】この発明が適用されたメモリカードの一例の説明に用いるフローチャートである。
【図１０】この発明が適用されたメモリカードの一例の説明に用いるフローチャートである。
【図１１】この発明が適用されたメモリカードの一例の説明に用いるフローチャートである。
【図１２】この発明が適用されたメモリカードの他の例のブロック図である。
【符号の説明】
３０９・・・シリアル／パラレル変換器、３１０・・・レジスタ、３１５・・・フラッシュメモリ、３１６・・・ＣＰＵ

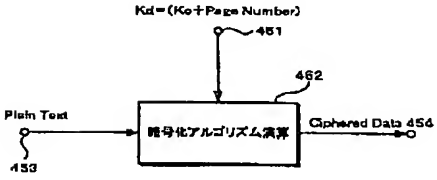
【図１】



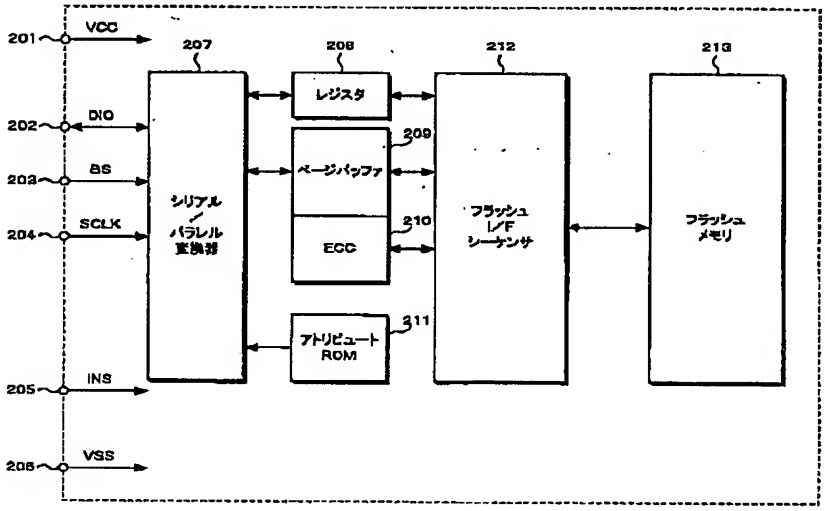
【図５】



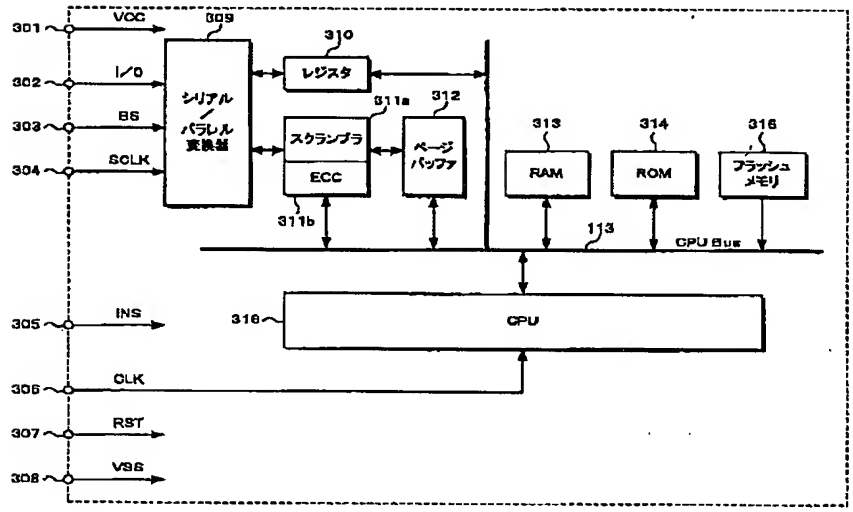
【図６】



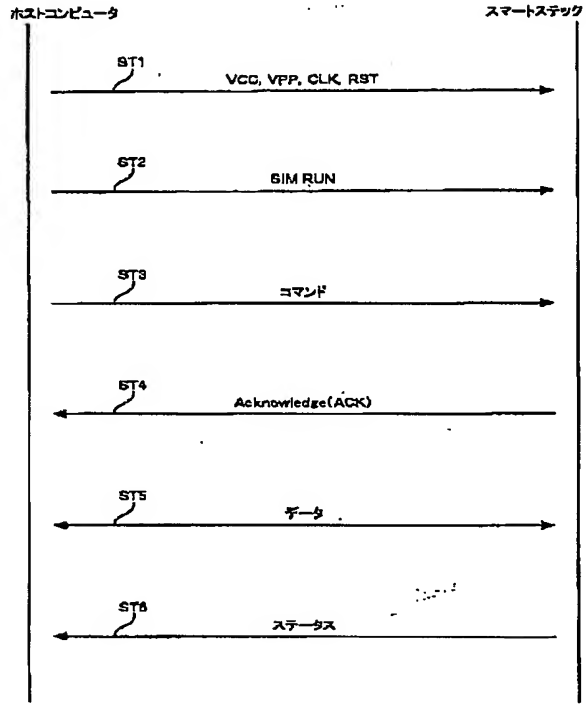
【図2】


201
VCC
207
208
212
213
202
DIO
レジスタ
209
ページバッファ
203
BS
シリアル/パラレル変換部
204
SCLK
210
ECC
フラッシュI/Fシーケンサ
フラッシュメモリ
311
アトリビュートROM
205
INS
206
VSS

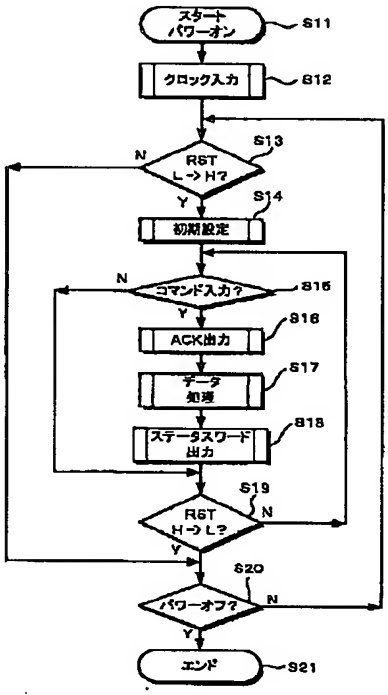
【図3】


301
VCC
309
310
302
I/O
レジスタ
シリアル/パラレル変換器
303
BS
311a
312
313
314
316
304
SCLK
スクランブラ
ECC
ページバッファ
RAM
ROM
フラッシュメモリ
311b
113
CPU Bus
305
INS
316
CPU
306
CLK
307
RST
308
VSS

【図4】



【図9】



【図7】

ディレクトリ デスクリプション

共通仕様

	Byte(s)	Description	Length
A	1-4	残存未使用Memory量	4
	5-20	Directory ID + Tag	16
	21	Directory Type	1
	22-27	Time Stamp(yyyy, MM, dd, hh, mm)Option	6
	28-29	RFU	2
	30	次に続くApplication用のFile Data長	1

各Application用の仕様

	Byte(s)	Description	Length
B	31	Directory Characteristics	1
	32-33	Sub-Directory数	2
	34-35	現状Directory下のFile数	2
	36	PIN, Unblocking PIN, Administrative Code 数	1
	37	RFU	1
	38	PIN 1 Status	1
	39	Unblocking PIN 1 Status	1
	40	PIN 2 Status	1
	41	Unblocking PIN 2 Status	1
	42-46	Administrative Management Use	7

C
Directory Type Coding(例)
00:RFU
01:Directory
02:Sub-Directory
04:Data File

D
Directory Characteristics(例)
Bit 1:Clock Stop Mode
Bit 2:RFU
Bit 3-4:Clock Stop Mode
Bit 5-7:RFU
Bit 8:PIN 1 有効/無効

E
Security Status(例)
Bit 1-4:PIN誤入力Counter
0はBlockされている事を示す。
Bit 5-7:RFU
Bit 8:初期化情報

【図8】

ファイル ディスクリプション

共通仕様

Byte(s)	Description	Length
1-4	File Size	4
5-20	File ID + Tag	16
21	File Type	1
22-27	Time Stamp(yyyy, MM, dd, hh, mm)Option	6
28	Mode	1
29-32	Access Conditions	4
33	File Status	1
34	次に続くApplication用のFile Data長	1

A

各Application用の仕様

Byte(s)	Description	Length
35	Structure of Data File	1
36-37	Length of Record	2

B

C
File Type Coding(例)
00:RFU
01:Directory
02:Sub-Directory
04:Data File

D
Mode(例)
INCREASE Command
Enable/Disable for Cyclic File

E
Mode(例)
Bit 1-7:RFU
Bit 8:INCREMENT Command Allowed or Not

F
Access Condition Code(例)
0:ALW(sys)
1:PIN 1
2:PIN 2
3:RFU
4:ADM(Interactive)
:
E:ADM
F:NEV(er)

Byte 29(例)
Bit 1-4:UPDATE
Bit 5-8:READ:SEEK

Byte 30(例)
Bit 1-4:RFU
Bit 5-8:INCREASE

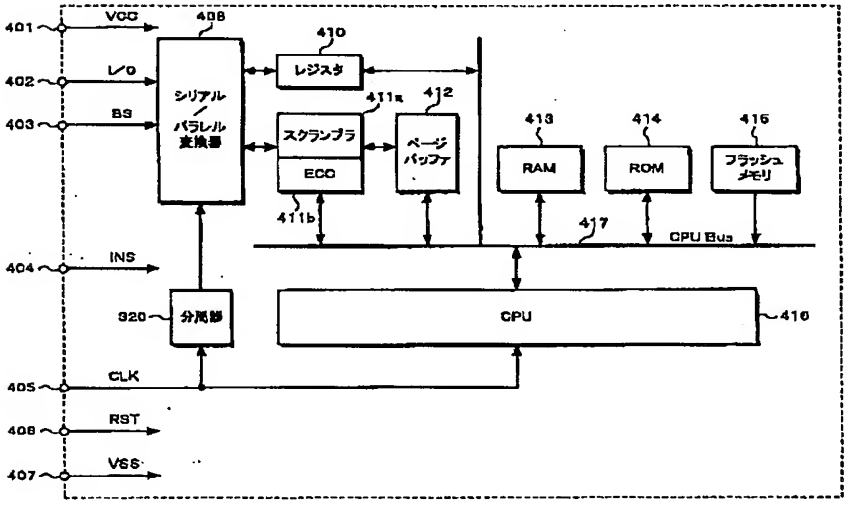
Byte 31(例)
Bit 1-4:INVALIDATE
Bit 5-8:REHABILITATE

Byte 32(例)
Bit 1-4:SCRAMBLE
Bit 5-8:COPY

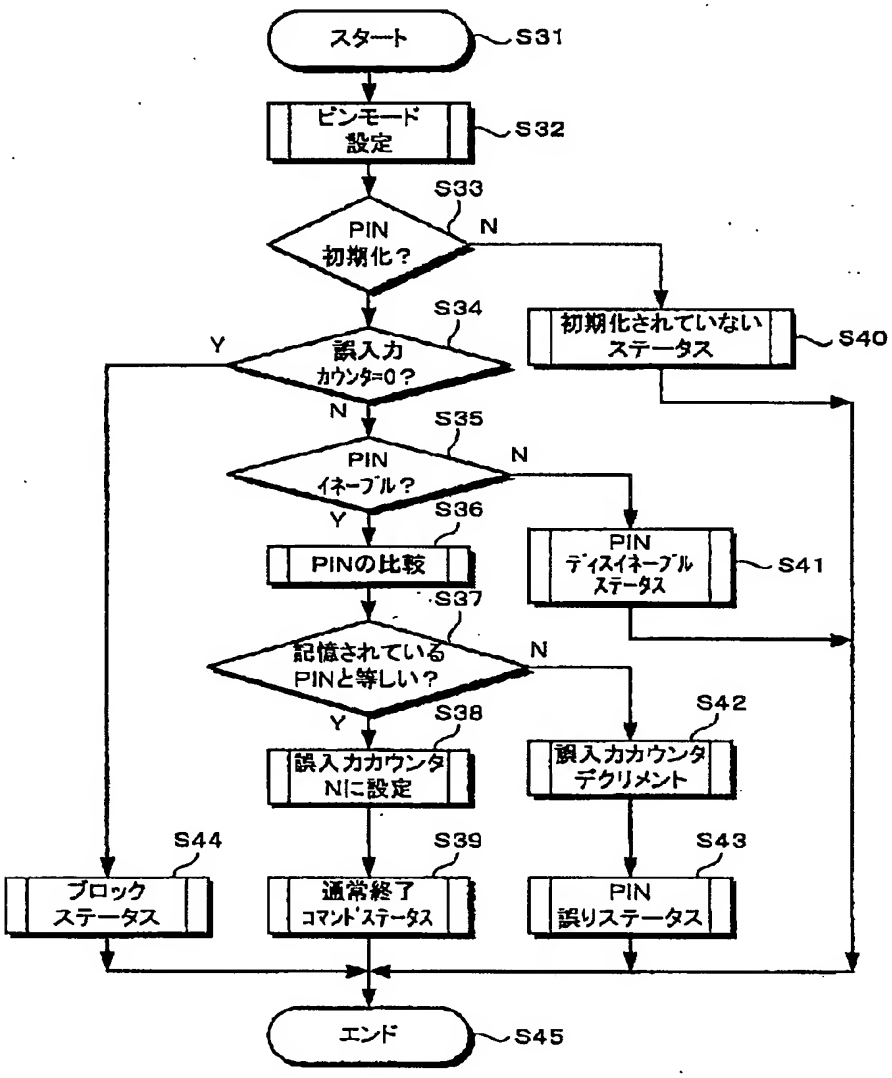
G
File Status(例)
Bit 1:Invalidated or Not
Bit 2:Scrambled or Not
Bit 3-8:RFU

File Structure(例)
00:Transparent
01:Linear Fixed
03:Cyclic

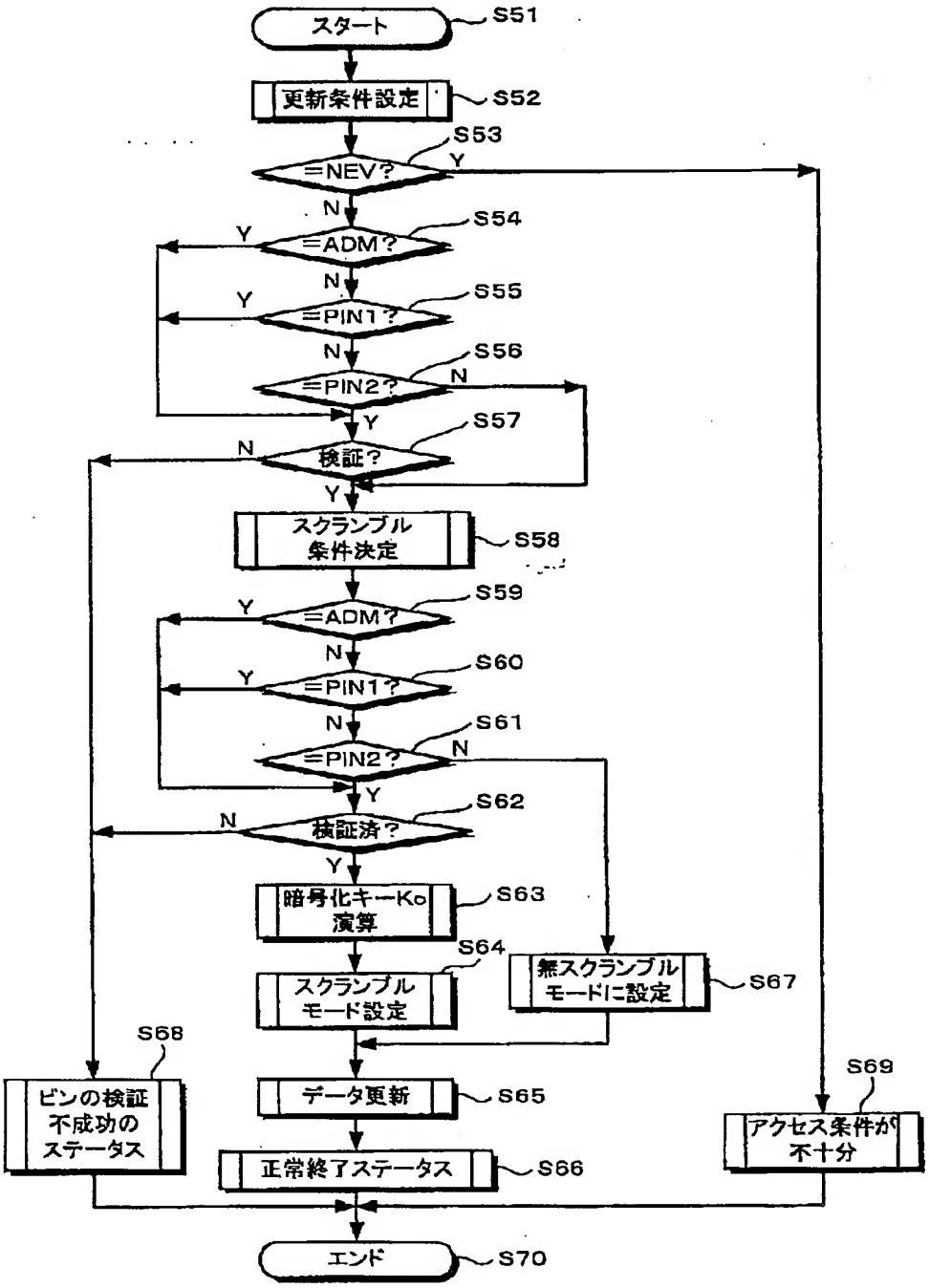
【図12】



【図10】


スタート
S31
ピンモード設定
S32
S33
PIN初期化？
N
Y
S34
誤入力カウンタ=0？
初期化されていないステータス
S40
N
S35
PINイネーブル？
N
Y
S36
PINの比較
PINディスイネーブルステータス
S41
S37
記憶されているPINと等しい？
N
Y
S38
S42
誤入力カウンタNに設定
誤入力カウンタデクリメント
S44
S39
S43
ブロックステータス
通常終了コマンドステータス
PIN誤りステータス
エンド
S45

【図11】


スタート
S51
更新条件設定
S52
S53
=NEV?
Y
N
S54
=ADM?
Y
N
S55
=PIN1?
Y
N
S56
=PIN2?
N
Y
S57
検証?
N
Y
スクランブル条件決定
S58
S59
=ADM?
Y
N
S60
=PIN1?
Y
N
S61
=PIN2?
N
Y
S62
検証済?
N
Y
暗号化キーKo演算
S63
S64
スクランブルモード設定
無スクランブルモードに設定
S67
S68
ビンの検証不成功のステータス
データ更新
S65
S69
アクセス条件が不十分
正常終了ステータス
S66
エンド
S70

フロントページの続き

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
Ｇ０６Ｆ 12/00	５３７	Ｇ０６Ｆ	12/00	５３７Ｍ
				５３７Ａ
				５３７Ｄ
Ｇ０６Ｋ 17/00		Ｇ０６Ｋ	17/00	Ｅ
19/073			19/00	Ｐ

Ｆターム(参考) 5B017 AA01 AA06 BA05 BA07 BB03
BB08 CA07 CA08 CA11 CA12
CA14 CA15 CA16
5B035 AA13 AA14 BB09 BC00 CA39
5B058 CA23 KA33 KA35 YA16
5B082 AA11 CA07 EA01 GA02 GA14
GC05 JA08